Small systems security guidelines

Government of Canada

Security

"Small Systems Security Guidelines"

Canada

Royal Canadian Mounted Police
Gendarmerie royale du Canada

In Consultation with others...

This is one of a series of publications on security published by the lead security agencies and central agencies in consultation with departments. The series is designed to help all departments meet the requirements and standards set out in the security policy and appendices.

Published by the RCMP in consultation with :

Treasury Board of Canada Secretariat
Communications Security Establishment
Information Technology Security Committee

Minister of Supply and Services Canada, 1992
Cat. No. BT32-36/7-1992
ISBN 0-662-59297-2

ISSN 1188-6315
Information Management Partnership Publishing

Small Systems Security Guidelines

October 1992

Table of Contents

1. OVERVIEW 1

1.1 Introduction 1
1.2 Background 1
1.3 Scope 2
1.4 Objective 3

2. DESIGNATED INFORMATION 5

2.1 Introduction 5
2.2 Administration and Organization 5
2.3 Personnel 7
2.4 Physical and Environmental 8
2.5 Hardware 10
2.6 Communications 11
2.7 Software 12
2.8 Operations 13

3. CLASSIFIED INFORMATION 17

3.1 Introduction 17
3.2 Administration and Organization 17
3.3 Personnel 17
3.4 Physical and Environmental 17
3.5 Hardware 18
3.6 COMSEC 19
3.7 Software 19
3.8 Operations 19

1. OVERVIEW

1.1 Introduction

Information technology (IT) security is the protection resulting from an integrated set of measures designed to ensure confidentiality of information electronically stored, processed or transmitted, the integrity of the information and the availability of systems and services. IT security standards have been developed to assist government organizations in implementing an effective IT security program. The document Technical Security Standards for Information Technology (TSSIT) addresses the "rings of security", i.e. (1) Organizational and Administrative, (2) Personnel, (3) Physical and Environmental, (4) Hardware, (5) Communications, (6) Software, and (7) Operations. TSSIT describes in detail the minimum security requirements that all computer systems must meet to protect data in accordance with its defined sensitivity.

The guidelines provided below have been extracted from TSSIT and modified to reflect use of new technologies in office environments where small systems are used. Many of the guidelines are not unique to such an environment, but have been consolidated here for the convenience of the user.

1.2 Background

A significant difference in the use of large computers and small systems is that responsibility for and operation of the large computers is assigned to data centre management, while small system users have control of and responsibility for all aspects of the system

operation. Personnel using small computer systems usually do not have an information processing background and thus are often not aware of the vulnerabilities associated with the use of small systems. Consequently, sensitive data on small systems may be inadequately protected.

Historically, protection of large computers, including the backup and recovery of data files, was the responsibility of data centre personnel. Theft of large systems or related peripherals, such as disks and tapes, was infrequent, primarily due to the physical size of these systems and the implementation of physical access controls at most data centres. With the current proliferation of computers in the office and the home, small systems are exposed to a new type of threat. The theft of the system components and media (diskettes & hard disks) is motivated not by the data contained therein but by the value and attractiveness of the hardware itself. Another security concern associated with the use of small systems, especially those connected to a network, is the difficulty in controlling the unauthorized expansion of hardware and software products which may compromise, either accidentally or deliberately, the security of the system or network. When using small computer systems, the users themselves are required to perform all system operational functions, including ensuring the security of the system and the data stored therein. Consequently, it is imperative that users be educated not only in the use of the systems but also in the importance of proper security procedures.

1.3 Scope

The major thrust of the government's IT security standards is aimed at minicomputers and

mainframe installations. Since microcomputer-based systems, such as personal computers and word processors, do not have or require all the capabilities of a general purpose system, not all IT security standards are applicable.

These guidelines are applicable to systems functioning either as stand-alone units or interconnected to other systems and operating within an office environment without requiring extraordinary physical and environmental (e.g. air conditioning, raised flooring, or power supply) or personnel (computer operators) support. This definition includes standard office automation equipment, such as microcomputers (personal computers) and word processors, as well as local area networks (LAN)s consisting of small systems and small systems acting as remote terminals to large computers and data networks. Additionally, for those small systems connected to large computers or data networks, the security standards of the "host" system must be adhered to and, consequently, from the "host perspective", the small system must comply with the security standards detailed in the IT standards. Also included in this definition are laboratory and science and engineering systems used in the collection and manipulation of sensitive specialized data.

1.4 Objective

The purpose of these guidelines is to assist organizations, management and users with the identification, development and implementation of administrative, technical and procedural safeguards which are required for the protection of information being processed on small computer systems. It must be emphasized, however, that these guidelines are general in

nature and will not cover all situations, equipment or types of interconnected systems. The degree of protection applied must be commensurate with the level of sensitivity of the information being processed or stored. A threat and risk assessment must be conducted to assess the threats and to develop cost-effective countermeasures. Departmental security staff can assist with this assessment process. These guidelines are meant to address security concerns of stand-alone, interconnected, and externally connected small computer systems.

2. DESIGNATED INFORMATION

2.1 Introduction

The guidelines in this chapter summarize the security measures required by organizations using small systems to process, store or transmit designated information. Chapter 3 contains additional safeguards for systems processing classified information.

2.2 Administration and Organization

1. Accountability for the security of each system/network should be assigned. These functional responsibilities should be defined, documented and distributed.

2. All hardware/software/communications additions, changes or deletions to the configuration of small systems and/or the network should be authorized by the individual responsible for the system and/or network.

3. System security policies, procedures and standards should be developed, documented and distributed.

4. The confidentiality, criticality of service, and backup requirements of the programs and data processed should be established in a "Statement of Sensitivity".

5. A threat and risk assessment shall be conducted.

6. Rules and regulations (to be "signed off" by system users) associated with access to the

system resources should be developed and stipulate:

- that system and data resources shall be used only in direct support of authorized projects, together with explicit exceptions if required;
- responsibilities (accountability) respecting the use of user-IDs, passwords and access control items such as encryption keying material, keys, locks, and card access;
- the authority required to modify, delete or add to sensitive data or programs;
- the authority required to access any data or program entity not specifically owned or controlled by the person wishing access;
- responsibilities respecting the confidentiality of information on or relating to the system;
- responsibilities respecting the restriction of use and/or copying of copyright-protected programs and data;
- restrictions which limit an individual's access to specific locations, times, systems, files and programs (transactions);
- the authority required to modify, delete or add hardware, software or communications components;
- responsibilities respecting the reporting of security infractions;
- the authority required to remove hardware, communications, or software products from the premises (both permanently and temporarily);
- responsibilities respecting the backup of critical programs and data;
- that all software and hardware be examined for malicious code, e.g. viruses, prior to initial use; and
- that any violation of the spirit or intent of the rules and regulations can lead to loss

of privilege or employment, disciplinary action or legal procedure.

7. Records should be maintained recording the signed acknowledgement of each individual who is to be authorized access to the system that the rules and regulations associated with such access have been read.

8. A security-incident-reporting procedure should be developed, documented and implemented. A definition of a security incident in the system environment should be developed.

9. Contingency plans for systems should be established.

10. An annual security audit of the small systems and network should be conducted.

2.3 Personnel

1. Enhanced reliability checks shall be conducted for all users who may have access to systems that process designated information.

2. A small computer systems security awareness program should be developed for users and include information concerning the security vulnerabilities associated with the use of small computer systems.

3. On termination or transfer of employment, procedures shall exist to:

   - revoke access privileges (e.g. user-IDs and passwords) to system and data resources,
   - retrieve sensitive material including access control items (e.g. keys and badges), and

- retrieve small systems-related hardware, software and documentation.

4. A need-to-know profile should be established for all users. It should specify the users' "access rights" in relation to information contained on the system or network.

2.4 Physical and Environmental

1. Where the storage media cannot be removed from the system, complementary physical and logical access control techniques should be implemented. Examples of these access controls are:

   - entrance doors to the system facility are at least secured with approved doors and locking hardware;
   - walls of the room housing the equipment are constructed from the floor to the real ceiling;
   - access to the system area is restricted to authorized personnel;
   - access to the system area is secured in the absence of personnel authorized for the system;
   - signs to demarcate the appropriate secure zone (e.g. Operations Zone) are prominently posted at all entrances to a facility (room) housing a number of the systems;
   - surveillance methods, such as motion detectors and alarms, are implemented for the area housing the equipment;
   - the entire system is stored in an appropriate security container when not in use; and
   - logical access to system resources is controlled using techniques such as encryption, passwords, and hardware/ software access controls.

2. Where removable media is used to store designated information:

   - the media should be stored in an appropriate security container when not in use; and
   - where confidentiality is a concern, the information should be encrypted.

3. All designated information, whether it be on magnetic media or hardcopy documents, should be controlled whenever the system equipment is left unattended.

4. Where processed information is particularly sensitive, procedures for securing printer ribbons should be documented and implemented. Printer ribbons, OPC cartridges, laser printer cartridges, and carbon paper should be:

   - physically secured during silent hours and controlled when the printer is left unattended;
   - disposed of in an approved manner (e.g. by burning or shredding); and
   - suitably protected, including inventory control, while awaiting destruction.

5. Procedures should be implemented for the disposal of sensitive hardcopy waste by such means as shredding, mulching or burning.

6. Procedures should be implemented for the disposal of sensitive magnetic media (hard disk, floppy diskettes, magnetic tapes, optical disks) by such means as overwriting, degaussing or burning.

7. Provisions for physical security at offsite storage facilities should be commensurate with that required at the primary site.

8. Where unauthorized removal of the system or its components is a concern, the system should be secured by the implementation of additional security measures.

2.5 Hardware

1. An inventory of all small systems should be maintained indicating the unique identification of the system and components, the location, and the individual responsible.

2. An institutional standard hardware configuration should be established and maintained.

3. Unless access to particularly sensitive data is deemed impossible, hardware maintenance personnel should be supervised by a knowledgeable person who understands the implications of the actions taken.

4. Where equipment maintenance requires the exchange or release of components (tapes, disks, diskettes, memory, EPROMS) which may contain sensitive information, those components should not be released to the vendor unless the data has been rendered unintelligible by means of approved erasure or encryption. Where these methods cannot be used, the equipment shall be disposed of using approved procedures.

5. A power surge suppressor should be installed in those localities which have a history of frequent significant power fluctuations.

6. Where static electricity may affect the integrity and reliability of the data and programs processed and stored on the

equipment, anti-static devices should be installed.

7. Records of all hardware modifications, configuration changes and maintenance activities should be retained for a period of one year.

8. To detect and prevent small systems from being infected by computer viruses, all newly acquired hardware, or hardware returned from maintenance, should be scanned for the existence of viruses.

2.6 Communications

1. For LANs, a configuration chart of the current data communications should be maintained.

2. Where sensitive data is processed or stored on a system, or on a system which is part of a network, all communications with that system or network should be controlled. Note: Techniques such as voice recognition, smart card, government-approved encryption, dial-back units, and controlled user groups are recognized means of controlled communications.

3. Where unauthorized access is a concern, all unsuccessful system access attempts should be recorded and reviewed.

4. When transmitting information where data integrity is a concern, an integrity code should be included with the data to verify that the data has not been altered during transmission.

5. When transmitting particularly sensitive information, government-approved cryptography or other approved COMSEC measures shall be used unless a threat and risk assessment indicates otherwise.

2.7 Software

1. A current inventory should be maintained of all software (copyrighted/licensed/developed) and important (or shared) information.

2. When users without a common need-to-know share a system, logical access controls should be implemented to ensure only authorized users are permitted access to the information.

3. Where systems or networks process information of differing sensitivities, the information should be stored on separate physical devices. Where this is not practical, or when particularly sensitive information is involved, government-approved encryption should be considered.

4. Where the user identification is authenticated, the user authentication information should not be displayed, and should be protected from unauthorized access.

5. Where data integrity is a concern, procedures should be implemented to ensure that:

   - changes to programs and data are authorized and controlled, and
   - acceptance tests are conducted.

6. Where data integrity is a concern, controls should be implemented to ensure that the

integrity is maintained while the data is stored or processed on the system. Examples of such controls include batch totals, file record counts, file release dates and version numbers, block counts, check sums, hash totals, data edit routines, and file and message authentication coding.

7. A system development life cycle (SDLC) methodology should be implemented where significant resources are used for the development of applications or, where warranted, due to the sensitivity of the data to be processed. The SDLC should ensure that:

   - security concerns are addressed,
   - test criteria are met prior to implementation of operational software,
   - change control procedures for operational software are implemented, and
   - discrepancies for all data and software are reported, monitored and resolved.

2.8 Operations

1. A physical inventory of all storage media containing designated information should be carried out at least annually.

2. Where user identification and authentication mechanisms are used, procedures should be implemented which:

   - control the issue, change, cancellation and audit of user identifiers and authentication mechanisms; and

- ensure that authentication codes or passwords are:
  - generated, controlled and distributed so as to maintain the confidentiality and availability of the authentication code;
  - known only to the authorized user of the account;
  - pseudo-random in nature or vetted through a verification technique designed to counter triviality and repetition;
  - no less than five characters in length;
  - one-way encrypted;
  - excluded from unprotected automatic log-on processes; and
  - changed at least annually.

3. To ensure integrity and availability of essential data and programs:

   - backup copies of the essential information should be taken at regular intervals; and
   - based on the criticality of the information and availability requirements, backup copies of the information should be stored at an offsite location.

4. All storage media containing designated information, whether removable or not, should:

   - be clearly marked to denote the highest designation stored on that media, and
   - retain its marking until:
     - all information on the media has been downgraded,
     - the media has been sanitized using an approved procedure, or
     - the media has been disposed of using an approved procedure.

5. Where confidentiality is a concern, system display units and hardcopy production units should be positioned or equipped with protective material, e.g. limited vision screens or printer covers, such that the information displayed or processed cannot be readily viewed by unauthorized persons.

6. Users of a system or network which processes sensitive information on non-removable media should be uniquely identified. This identification should be authenticated prior to users being given access to the system and data resources.

7. Where equipment is to be removed from the premises on a temporary basis, control procedures should be implemented and include:

   - the approval authority,
   - the identity of the borrower,
   - the equipment identification,
   - a signed acknowledgement of acceptance and return of equipment, and
   - a requirement to sanitize the equipment before and after the loan period.

8. Where confidentiality is a concern, the contents of erasable media should be obscured using an approved technique before the media is re-used.

9. Where confidentiality is a concern, automated and/or manual controls should be implemented to prevent unauthorized copying, transmission or printing.

10. Where data integrity is a concern, control procedures should be implemented to:

    - ensure information to be entered or processed has been duly authorized,

- verify the accuracy of the information,
- retain the identity of the individual(s) who authorized and entered the information, and
- maintain an audit trail of transactions entered on the system.

11. The system should maintain a log of all security-relevant activities on the system, e.g. logins and file accesses.

12. Procedures should be implemented to ensure that critical operational material and media resources are identified on a continuing basis to enable restoration of the minimum essential level of service following the loss of equipment or service.

13. To detect and prevent small systems from being infected by computer viruses, the following precautions should be observed:

    - all media received from external sources, including licensed or copyright software, should be scanned for the existence of viruses,
    - all original master copies of software should be stored on media with the write-protect security feature activated, and
    - computer systems should be scanned for the existence of viruses after software and hardware maintenance.

14. A contingency procedure should be developed detailing the course of action to be followed when a virus attack is suspected.

3. CLASSIFIED INFORMATION

3.1 Introduction

The guidelines in this chapter contain a summary of additional security measures required by organizations using small systems to process, store or transmit information classified Confidential or Secret in the national interest. Top Secret information will require protective measures in addition to those described in this chapter, and advice and guidance can be obtained from the Departmental Security Officer, SEIT and CSE.

3.2 Administration and Organization

Procedures should be developed, documented and implemented to ensure that:

1. the information is assigned a security classification,
2. the classification and declassification conform with the provisions of the Security Policy of the Government of Canada, and
3. appropriate security clauses specifying security requirements are included in all contractual arrangements with other organizations.

3.3 Personnel

Personnel who have access to classified information shall be security screened to the highest classification level of information accessed.

3.4 Physical and Environmental

1. Access to system and data resources where classified data is processed or stored should

be restricted to those having a common need-to-know.

2. The area housing a system on which classified information is stored on non-removable media should be secured in an approved manner.

3. The area housing TEMPEST-compliant small systems equipment should be secured.

4. Records should be kept of anyone accessing the area where the small systems containing classified information are located.

5. Procedures for the disposal of classified hardcopy, storage media, printer ribbons and OPC cartridges should comply with the Security Policy of the Government of Canada.

6. Areas where classified information is processed or stored should be established as a Security or a High Security Zone. Access privileges should be controlled and authorized.

7. Installations or modifications of TEMPEST-compliant small systems should be approved by the COMSEC authority.

3.5 Hardware

Where equipment maintenance requires the exchange or release of components (tapes, disks, diskettes, memory, EPROMS) which contain classified information, those components should not be released to the vendor unless the data has been rendered unintelligible by means of approved erasure techniques or encryption. Where this procedure cannot be used, the equipment shall be disposed of using approved procedures.

3. RENSEIGNEMENTS CLASSIFIÉS

3.1 Introduction

Les lignes directrices du présent chapitre contiennent un résumé des mesures de sécurité supplémentaires que les organisations qui utilisent des petits systèmes doivent mettre en oeuvre pour traiter, emmagasiner ou transmettre les renseignements classifiés «confidentiel ou secret» dans l'intérêt national. Les renseignements «très secret» nécessiteront des mesures de protection additionnelles, en plus de celles décrites dans le présent chapitre; on peut obtenir des conseils et des avis de l'agent de sécurité du ministère, de l'Équipe d'inspection et d'évaluation de la sécurité (ÉIÉS) et du Centre de la sécurité des télécommunications (CST).

3.2 Administration et organisation

On devrait élaborer des procédures, les documenter et les mettre en oeuvre afin que:

1. l'on attribue une classification de sécurité à l'information;
2. la classification et la déclassification soient conformes aux dispositions de la Politique du gouvernement du Canada sur la sécurité;
3. des clauses appropriées précisant les exigences en matière de sécurité soient incluses dans tous les arrangements contractuels conclus avec d'autres organisations.

3.3 Personnel

Le personnel qui a accès aux renseignements classifiés doit faire l'objet d'un filtrage de sécurité au plus haut niveau de classification des renseignements auxquels il a accès.

3.4 Sécurité matérielle et du milieu

1. Lorsque des renseignements classifiés sont traités ou emmagasinés, l'accès aux systèmes et aux ressources en information devrait être limité aux personnes qui ont le même besoin de savoir.

2. La zone abritant un système dans lequel des renseignements classifiés sont conservés sur des supports non amovibles devrait être protégée selon une méthode approuvée.

3. La zone qui abrite l'équipement des petits systèmes TEMPEST devrait être protégée.

4. On devrait tenir des registres de toutes les personnes qui ont accès à la zone où les petits systèmes contenant des renseignements classifiés sont situés.

5. Les procédures relatives à la destruction de documents sur papier, de supports d'entreposage, de rubans d'imprimantes et de cartouches de contrôle opérateur devraient être conformes à la Politique du gouvernement du Canada sur la sécurité.

6. Les zones dans lesquelles les renseignements classifiés sont traités ou conservés devraient être considérées comme des zones d'accès restreint (sécurité ou haute sécurité). Les privilèges d'accès devraient être contrôlés et autorisés.

7. Les installations ou les modifications des petits systèmes TEMPEST devraient être approuvées par le responsable COMSEC.

- retain its marking until:
  - all information on the media has been declassified,
  - the media has been sanitized using an approved procedure, or
  - the media has been disposed of using an approved procedure.

5. When changing modes of operation (usually caused by change of common need-to-know, classification, or access rights), the following procedures are to be implemented:

   - data communication lines should be controlled,
   - memory should be sanitized,
   - access paths to data should be established as required, and
   - a fresh copy of an appropriately protected version of the operating system should be utilized.

3. Pour assurer l'intégrité et la disponibilité des données et des programmes essentiels:

   - des copies de sauvegarde des renseignements essentiels devraient être conservées à intervalles réguliers;
   - compte tenu de l'importance critique de l'information et des exigences concernant la disponibilité, des copies de sauvegarde des renseignements devraient être conservées dans une installation auxiliaire.

4. Tous les supports d'entreposage contenant des renseignements classifiés, amovibles ou non, devraient:

   - être clairement identifiés de façon à indiquer la classification de sécurité la plus élevée des renseignements conservés sur ce support;
   - conserver leur identification jusqu'à ce que:
     - toute l'information contenue sur le support ait été déclassifiée;
     - le support ait été validé au moyen d'une procédure approuvée;
     - le support ait été détruit au moyen d'une procédure approuvée.

5. Au moment de modifier les modes d'exploitation (habituellement parce que le même besoin de savoir, la classification ou les droits d'accès ont été modifiés), on doit mettre en oeuvre les procédures suivantes:

   - contrôler les lignes de transmission des données;
   - valider la mémoire;
   - établir au besoin des cheminements d'accès aux données;
   - utiliser une nouvelle copie d'une version protégée appropriée du système d'exploitation.

3.8 Opérations

1. Un inventaire de tous les supports d'entreposage contenant des renseignements classifiés devrait être effectué au moins selon le calendrier suivant:

Très secret	–	une fois par mois
Secret	–	une fois par trimestre
Confidentiel	–	une fois par trimestre

2. Lorsque les mécanismes d'identification et d'authentification des usagers sont utilisés, on devrait mettre oeuvre des procédures qui permettent de:

   - contrôler l'établissement, le changement, l'annulation et la vérification des mécanismes d'identification et d'authentification des usagers;
   - s'assurer que les codes d'authentification ou les mots de passe sont:
     - produits, contrôlés et distribués de façon à conserver la confidentialité et la disponibilité du code d'authentification;
     - connus uniquement de l'usager autorisé du compte;
     - pseudo-sélectifs de nature, ou validés au moyen d'une technique de vérification conçue pour éviter la banalisation et la répétition;
     - composés d'au moins cinq caractères;
     - à chiffrement unidirectionnel;
     - exclus des procédés d'entrée en communication automatiques non protégés;
     - modifiés conformément au tableau suivant:

confidentiel	–	une fois par trimestre
secret	–	une fois par trimestre
très secret	–	une fois par mois

3.5 Matériel

Lorsque l'entretien de l'équipement nécessite l'échange ou le retrait de composantes (bandes, disques, disquettes, mémoire, EPROM) qui contiennent des renseignements classifiés, ces composantes ne devraient pas être transmises au fournisseur à moins que les données aient été rendu méconnaissables au moyen de techniques d'effacement ou de chiffrement approuvées. Lorsqu'il est impossible d'utiliser ces techniques, l'équipement doit être détruit à l'aide de procédures approuvées.

3.6 COMSEC

1. On doit utiliser uniquement de l'équipement TEMPEST ou d'autres méthodes approuvées pour traiter les renseignements classifiés, à moins qu'une évaluation des menaces et des risques n'indique autrement.

2. Au moment de communiquer des renseignements classifiés, on doit protéger l'information contre toute divulgation non autorisée au moyen de méthodes de chiffrement approuvées ou d'autres mesures approuvées COMSEC.

3.7 Logiciel

1. L'accès aux systèmes et aux ressources en information devrait être limité aux personnes qui ont le même besoin de savoir et des privilèges d'accès communs.

2. Tous les changements apportés aux programmes devraient être autorisés et contrôlés.

- ensure that authentication codes or passwords are:
  - generated, controlled and distributed so as to maintain the confidentiality and availability of the authentication code;
  - known only to the authorized user of the account;
  - pseudo-random in nature or vetted through a verification technique designed to counter triviality and repetition;
  - no less than five characters in length;
  - one-way encrypted;
  - excluded from unprotected automatic log-on processes; and
  - changed in accordance with the following minimum schedule:

Confidential	–	Quarterly
Secret	–	Quarterly
Top Secret	–	Monthly

3. To ensure integrity and availability of essential data and programs:

   - backup copies of the essential information should be taken at regular intervals; and
   - based on the criticality of the information and availability requirements, backup copies of the information should be stored at an offsite location.

4. All storage media containing classified information, whether removable or not, should:

   - be clearly marked to denote the highest security classification stored on that media, and

3.6 COMSEC

1. Only TEMPEST-compliant equipment or other approved methods shall be used to process classified information, unless a threat and risk assessment indicates otherwise.

2. When communicating classified information, the information shall be protected against unauthorized disclosure by approved cryptography or other approved COMSEC measures.

3.7 Software

1. Access to system and data resources should be restricted to persons having a common need-to-know and common access privileges.

2. All changes to programs should be authorized and controlled.

3.8 Operations

1. A physical inventory of all storage media containing classified information should be carried out in accordance with the following minimum schedule:

Top Secret	–	Monthly
Secret	–	Quarterly
Confidential	–	Quarterly

2. Where user identification and authentication mechanisms are used, procedures should be implemented which:

   - control the issue, change, cancellation and audit of user identifiers and authentication mechanisms; and

11. Le système devrait contenir un registre de toutes les activités liées à la sécurité dans le système, par exemple les entrées en communication et les accès aux fichiers.

12. On devrait mettre en oeuvre des procédures afin que le matériel d'exploitation essentiel et les ressources en supports soient identifiés en permanence pour permettre le rétablissement du niveau de service essentiel minimum en cas de perte d'équipement ou de service.

13. Pour déceler les virus informatiques et pour empêcher que les petits systèmes soient infectés, on devrait prendre les précautions suivantes:

    - tous les supports provenant de sources externes, y compris les logiciels protégés par une licence ou par un droit d'auteur, devraient être vérifiés afin de déceler s'ils contiennent des virus;
    - tous les exemplaires initiaux des logiciels devraient être conservés sur des supports et le système de sécurité visant à protéger l'écriture devrait être activé;
    - après l'entretien du logiciel et du matériel, on devrait vérifier les systèmes informatiques afin de déceler la présence de virus.

14. On devrait élaborer une procédure d'urgence précisant en détail la marche à suivre lorsque l'on prévoit une attaque de virus.

identifiés de façon spéciale. Cette identification devrait être authentifiée avant que l'on donne aux usagers l'accès au système et aux ressources en information.

7. Lorsque l'équipement doit être retiré temporairement des locaux, on devrait suivre des procédures de contrôle qui comprennent:

   - l'autorisation;
   - l'identité de l'emprunteur;
   - l'identification de l'équipement;
   - un document signé confirmant l'acceptation et le retour de l'équipement;
   - la nécessité de valider l'équipement avant et après la période du prêt.

8. Lorsque le caractère confidentiel des documents pose un problème, le contenu des supports effaçables devrait être obscurci à l'aide d'une technique approuvée avant que le support ne puisse être utilisé de nouveau.

9. Lorsque l'on se soucie de la confidentialité, on devrait mettre en oeuvre des contrôles automatisés ou manuels, ou les deux, pour prévenir le copiage, la transmission ou l'impression non autorisés.

10. Lorsque l'intégrité des données pose un problème, on devrait mettre en oeuvre des procédures de contrôle qui permettent de:

    - s'assurer que l'information qui doit être enregistrée ou traitée a été dûment autorisée;
    - vérifier l'exactitude de l'information;
    - conserver l'identité de la(des) personne(s) qui ont autorisé et enregistré l'information;
    - conserver une piste de vérification des transactions enregistrées dans le système.

3. Pour assurer l'intégrité et la disponibilité des données et des programmes essentiels:

   - on devrait faire une sauvegarde des renseignements essentiels à intervalles réguliers;
   - compte tenu de l'importance des renseignements et des exigences concernant la disponibilité, on devrait conserver les copies de sauvegarde des renseignements dans un emplacement auxiliaire.

4. Tous les supports d'entreposage contenant des renseignements désignés, amovibles ou non, devraient:

   - être clairement identifiés de façon à tenir compte des renseignements ayant la cote de sécurité la plus élevée sur ce support;
   - conserver leur identification jusqu'à ce que:
     - tous les renseignements emmagasinés sur le support soient déclassés;
     - le support ait été validé à l'aide d'une procédure approuvée;
     - le support ait été détruit à l'aide d'une procédure approuvée.

5. Lorsque l'on se préoccupe de la confidentialité, les unités d'affichage du système et les unités de production des supports rigides devraient être positionnées de façon appropriée ou équipées de matériel protecteur, par exemple des écrans de visualisation restreints ou des couvercles d'imprimantes, de façon que l'information affichée ou traitée ne puisse être vue facilement par des personnes non autorisées.

6. Les usagers d'un système ou d'un réseau qui traite des renseignements de nature délicate sur des supports non amovibles devraient être

- les écarts relatifs à toutes les données et à tous les logiciels sont déclarés, contrôlés et comblés.

2.8 Opérations

1. Un inventaire de tous les supports d'entreposage contenant des renseignements désignés devrait être effectué au moins une fois par an.

2. Lorsque les mécanismes d'identification et d'authentification de l'usager sont utilisés, on devrait mettre en oeuvre des procédures qui permettent:

   - de contrôler l'établissement, le changement, l'annulation et la vérification des mécanismes d'identification et d'authentification des usagers;
   - d'assurer que les codes d'authentification ou les mots de passe sont:
     - produits, contrôlés et distribués de façon à assurer la confidentialité et la disponibilité du code d'authentification;
     - connus uniquement de l'usager autorisé du compte;
     - pseudo-sélectifs de nature ou validés au moyen d'une technique de vérification conçue pour empêcher la banalisation et la répétition;
     - d'au moins cinq caractères;
     - à chiffrement unidirectionnel;
     - exclus des procédés d'entrée en communication automatiques non protégés;
     - modifiés au moins une fois par an.

4. Lorsque l'identité de l'usager est authentifiée, l'information à cet égard ne devrait pas être affichée et devrait être protégée de tout accès non autorisé.

5. Lorsque l'on s'inquiète de l'intégrité des données, on devrait suivre des procédures pour:

   - autoriser et contrôler les changements de programmes et de données;
   - effectuer des tests de réception.

6. Lorsque l'on se préoccupe de l'intégrité des données, on devrait mettre en oeuvre des contrôles afin de s'assurer que l'intégrité est protégée pendant que les données sont emmagasinées ou traitées dans le système. Parmi ces contrôles citons par exemple les totaux de lots, les comptes de fichiers, les dates de libération du volume du fichier et les numéros de version, les comptages de blocs, les totaux de contrôle, les programmes d'édition et les codes d'authentification des fichiers et des messages.

7. On devrait établir une méthode concernant la durée de vie utile de l'élaboration de systèmes lorsque des ressources considérables sont utilisées pour l'élaboration d'applications ou, lorsqu'il est justifié de le faire à cause de la nature délicate des données à traiter. La méthode susmentionnée devrait permettre de s'assurer que:

   - les inquiétudes concernant la sécurité sont apaisées;
   - les critères des tests sont satisfaits avant la mise en service du logiciel d'exploitation;
   - les procédures de contrôle des changements pour le logiciel d'exploitation sont mises en oeuvre;

4. Lorsque l'on se soucie de l'intégrité des données au moment de transmettre l'information, on devrait inclure un code d'intégrité avec les données, afin de s'assurer qu'elles n'ont pas été modifiées pendant la transmission.

5. Au moment de transmettre de l'information de nature particulièrement délicate, on doit utiliser la méthode de chiffrement approuvée par le gouvernement ou d'autres mesures approuvées COMSEC à moins qu'une évaluation des menaces et des risques n'indique autrement.

2.7 Logiciels

1. On devrait tenir à jour un inventaire de tous les logiciels (protégés par un droit d'auteur ou par une licence ou mis au point) et de toute l'information importante (ou partagée).

2. Lorsque des usagers qui n'ont pas le même besoin de savoir partagent un système, les contrôles de l'accès logique devraient être établis de façon à ce que seulement les usagers autorisés puissent avoir accès à l'information.

3. Lorsque les systèmes ou les réseaux traitent de l'information plus ou moins délicate selon le cas, l'information devrait être emmagasinée sur des supports matériels différents. Lorsqu'il n'est pas pratique de suivre cette directive, ou lorsque de l'information de nature particulièrement délicate est concernée, on devrait avoir recours à la méthode de chiffrement approuvée par le gouvernement.

6. Lorsque l'électricité statique risque de compromettre l'intégrité et la fiabilité des données et des programmes traités et entreposés dans l'équipement, on devrait installer des dispositifs anti-statiques.

7. On devrait conserver pendant un an les registres de toutes les modifications de matériel, des changements de configuration et des activités d'entretien.

8. Afin de déceler les virus et d'empêcher que les petits systèmes soient infectés, on devrait vérifier tout le matériel nouvellement acquis, ou le matériel qui vient de faire l'objet de travaux d'entretien.

2.6 Communications

1. Pour les réseaux locaux, on devrait tenir à jour un graphique de la configuration des communications actuelles de données.

2. Lorsque des données de nature délicate sont traitées ou emmagasinées dans un système, ou dans un système qui fait partie d'un réseau, on devrait contrôler toutes les communications avec ce système ou ce réseau. Note: Les techniques comme la reconnaissance vocale, les cartes à mémoire, le chiffrement approuvé par le gouvernement, les unités à fonction de rappel et les groupes d'usagers contrôlés sont des moyens reconnus de communications contrôlées.

3. Lorsque l'accès non autorisé pose un problème, on devrait enregistrer et examiner toutes les tentatives échouées d'accès au système.

8. Lorsque le retrait non autorisé du système ou de ses composantes pose un problème, le système devrait être protégé par des mesures de sécurité supplémentaires.

2.5 Matériel

1. On devrait tenir à jour un inventaire de tous les petits systèmes, en indiquant l'identification unique du système et de ses composantes, l'emplacement et la personne responsable.

2. On devrait établir et tenir à jour une configuration normalisée du matériel de l'institution.

3. À moins que l'accès aux données de nature particulièrement délicate soit considéré impossible, le personnel préposé à l'entretien du matériel devrait être supervisé par une personne qualifiée qui comprend les répercussions des mesures qui sont prises.

4. Lorsque l'entretien de l'équipement nécessite l'échange ou le retrait de composantes (bandes, disques, disquettes, mémoire, EPROM) qui peuvent contenir de l'information de nature délicate, on ne devrait pas remettre ces composantes au fournisseur à moins que les données aient été rendues méconnaissables au moyen de techniques approuvées d'effacement ou de chiffrement. Lorsqu'il est impossible d'utiliser ces méthodes, l'équipement doit être détruit conformément aux techniques approuvées.

5. On devrait installer un stabilisateur d'alimentation électrique dans les localités où il se produit souvent des variations de courant importantes.

3. Tous les renseignements désignés, conservés sur un support magnétique ou sur un support papier, devraient être contrôlés quand l'équipement est laissé sans surveillance.

4. Lorsque l'information traitée est de nature particulièrement délicate, on devrait documenter et mettre en application des procédures pour protéger les rubans d'imprimante. Les rubans d'imprimantes, les cartouches de contrôle opérateur, les cartouches d'imprimantes au laser et le papier carbone devraient être:

   - protégés en dehors des heures de travail et contrôlés lorsque l'imprimante est laissée sans surveillance;
   - éliminés de façon appropriée (par exemple, en les brûlant ou en les déchiquetant);
   - dûment protégés, y compris par le biais d'un contrôle de l'inventaire, en attendant la destruction.

5. On devrait mettre en oeuvre des procédures pour la destruction des imprimés de nature délicate en les déchiquetant, en les désintégrant ou en les brûlant.

6. On devrait mettre en oeuvre des procédures pour la destruction des supports magnétiques contenant de l'information de nature délicate (disque dur, disquettes souples, bandes magnétiques, disques optiques) en superposant l'écriture, en les démagnétisant ou en les brûlant.

7. Les dispositions en matière de sécurité du matériel dans les entrepôts auxiliaires devraient être équivalentes à celles établies pour l'emplacement principal.

de l'accès logique. Voici quelques exemples de ces contrôles d'accès:

- l'entrée qui donne accès au système est au moins protégée par des portes et des serrures approuvées;
- les murs de la pièce où se trouve l'équipement sont des murs de dalle à dalle;
- l'accès à la zone informatique est restreint au personnel autorisé;
- l'accès à la zone informatique est protégé en l'absence du personnel autorisé;
- des signaux sont affichés bien en évidence pour démarquer la zone d'accès restreint concernée (par exemple, zone des opérations) à toutes les entrées d'une installation (pièce) abritant des systèmes;
- des dispositifs de surveillance, par exemple des détecteurs de mouvement et des systèmes d'alarme, sont installés dans la zone où se trouve l'équipement;
- tout le système est entreposé dans un coffre sécuritaire adéquat lorsqu'il n'est pas utilisé;
- l'accès logique aux ressources du système est contrôlé à l'aide de techniques comme le chiffrement, les mots de passe et les contrôles d'accès au matériel et au logiciel.

2. Lorsque l'on utilise des supports amovibles pour entreposer des renseignements désignés:

   - le support doit être entreposé dans un coffre sécuritaire approprié lorsqu'il n'est pas utilisé;
   - lorsque le caractère confidentiel pose un problème, l'information devrait être chiffrée.

2.3 Personnel

1. On doit effectuer des vérifications approfondies de la fiabilité des usagers qui peuvent avoir accès aux systèmes qui traitent des renseignements désignés.

2. À l'intention des usagers, on devrait mettre en oeuvre un programme pour les sensibiliser à la sécurité des petits systèmes informatiques et pour leur indiquer jusqu'à quel point ces derniers sont vulnérables.

3. Lors d'une cessation d'emploi ou d'une mutation, on doit suivre des procédures pour:

   - révoquer les privilèges d'accès (par exemple, les cartes d'identité des usagers et les mots de passe) aux systèmes et aux ressources en information;
   - récupérer le matériel de nature délicate, y compris les instruments servant au contrôle de l'accès (par exemple, les clés et les insignes);
   - récupérer le matériel, le logiciel et la documentation des petits systèmes.

4. On devrait préciser ce que tous les usagers ont besoin de savoir, ainsi que leurs «droits d'accès» concernant l'information contenue dans le système ou dans le réseau.

2.4 Sécurité matérielle et du milieu

1. Lorsque le support d'entreposage ne peut être retiré du système, on devrait mettre en oeuvre des techniques de contrôle complémentaires de l'accès au matériel et

- l'autorisation requise pour modifier, supprimer ou ajouter des composantes au matériel, aux logiciels ou aux communications;
- les responsabilités concernant la déclaration des infractions à la sécurité;
- l'autorisation requise pour retirer (en permanence et temporairement) du matériel, des communications ou des logiciels des installations informatiques;
- les responsabilités concernant la sauvegarde des programmes et des données essentiels;
- la nécessité d'examiner les logiciels et le matériel afin de déceler les parasites, par exemple les virus, avant l'utilisation initiale;
- toute infraction aux règles et aux règlements peut donner lieu à une perte de privilèges ou d'emploi, à des mesures disciplinaires ou à des poursuites judiciaires.

7. Chaque personne qui doit être autorisée à avoir accès au système devrait d'abord signer un registre pour confirmer qu'elle a lu les règles et les règlements à cet égard.

8. On devrait établir, documenter et mettre en oeuvre une procédure concernant le rapport des infractions à la sécurité. Il faudrait aussi définir en quoi consiste une infraction à la sécurité dans l'installation informatique.

9. On devrait établir des plans d'urgence concernant les systèmes.

10. Chaque année, il faudrait vérifier la sécurité des petits systèmes et du réseau.

5. On doit évaluer les menaces et les risques.

6. Les règles et les règlements (que les usagers devront signer après en avoir pris connaissance) concernant l'accès aux ressources du système devraient stipuler ce qui suit:

   - les systèmes et les ressources en information doivent être utilisés uniquement pour appuyer directement les projets autorisés, et dans certains cas exceptionnels explicites, s'il y a lieu;
   - les responsabilités (responsabilisation) concernant l'utilisation des cartes d'identité des usagers, des mots de passe et des instruments permettant de contrôler l'accès, comme le matériel de perforation servant au chiffrement, les clés, les serrures et l'accès à l'aide d'une carte;
   - l'autorisation requise pour modifier, supprimer ou ajouter des données ou des programmes de nature délicate;
   - l'autorisation requise pour avoir accès à toute entité de données ou de programmes qui n'appartient pas expressément ou qui n'est pas contrôlée par la personne qui demande l'accès;
   - les responsabilités concernant le caractère confidentiel de l'information contenue dans le système ou de l'information connexe;
   - les responsabilités concernant la restriction de l'utilisation ou de la copie des programmes et des données protégés par un droit d'auteur, ou les deux;
   - les restrictions qui limitent l'accès d'une personne à des lieux, à des heures, à des systèmes, à des dossiers et à des programmes précis (transactions);

2. RENSEIGNEMENTS DÉSIGNÉS

2.1 Introduction

Les lignes directrices contenues dans ce chapitre résument les mesures de sécurité que doivent suivre les organisations qui utilisent des petits systèmes pour traiter, emmagasiner ou transmettre des renseignements désignés. Le chapitre 3 contient des mesures de protection supplémentaires pour les systèmes qui traitent les renseignements classifiés.

2.2 Administration et organisation

1. La responsabilité de la sécurité de chaque système ou réseau devrait être assignée à une personne en particulier. Ces responsabilités fonctionnelles devraient être établies, documentées et distribuées.

2. La personne responsable du système ou du réseau, ou des deux, devrait autoriser tous les ajouts, les changements ou les retraits de matériel, de logiciel et de communications concernant la configuration des petits systèmes ou du réseau, ou des deux.

3. Les politiques, les procédures et les normes en matière de sécurité devraient être établies, documentées et distribuées.

4. Le caractère confidentiel, l'importance du service et les exigences concernant la sauvegarde des programmes et des données traitées devraient être précisés dans un «Énoncé de la nature délicate des renseignements».

normes de sécurité énoncées dans les normes en matière de TI. Cette définition comprend également les systèmes utilisés dans les laboratoires et pour les travaux en sciences et en génie, c'est-à-dire pour recueillir et traiter des données spécialisées de nature délicate.

1.4 Objectif

Ces lignes directrices ont pour but d'aider les organisations, les gestionnaires et les usagers à identifier, à élaborer et à mettre en oeuvre les mesures de protection nécessaires sur le plan de l'administration, des exigences techniques et des procédures pour protéger l'information traitée à l'aide des petits systèmes informatiques. Il convient toutefois d'insister sur le fait que ces lignes directrices sont générales et ne couvrent pas toutes les situations, ni tout l'équipement, ni tous les types de systèmes interreliés. Le niveau de protection doit être choisi en fonction de la nature plus ou moins délicate de l'information traitée ou emmagasinée. On doit évaluer les menaces et les risques afin de pouvoir mettre en oeuvre des mesures correctrices ayant un bon rapport coût-efficacité. Le personnel responsable de la sécurité dans les ministères peut collaborer à ce processus d'évaluation.

Ces lignes directrices visent à régler les problèmes de sécurité que posent les petits systèmes informatiques autonomes, interreliés et liés à des réseaux de l'extérieur.

exercer eux-mêmes toutes les fonctions opérationnelles, y compris assurer la sécurité du système et des données qui y sont emmagasinées. Il est donc impératif d'apprendre aux usagers non seulement les règles de l'utilisation des systèmes mais aussi l'importance de suivre des procédures de sécurité appropriées.

1.3 Étendue

Les normes gouvernementales en matière de TI visent principalement les mini-ordinateurs et les unités centrales. Étant donné que les systèmes des micro-ordinateurs, par exemple, ceux des ordinateurs personnels et des machines de traitement de texte, n'ont pas toutes les capacités d'un système polyvalent ou n'en ont pas besoin, les normes de sécurité concernant la TI ne s'appliquent pas toutes.

Ces lignes directrices s'appliquent aux systèmes qui fonctionnent de façon autonome ou en étant reliés à d'autres systèmes, et qui sont exploités dans un bureau sans nécessiter de milieu ambiant extraordinaire (par exemple, climatisation de l'air, soulèvement du plancher ou alimentation en électricité) ni de personnel (opérateurs). Cette définition désigne l'équipement de bureautique courant, comme les micro-ordinateurs (ordinateurs personnels) et les machines de traitement de texte, ainsi que les réseaux locaux qui comprennent des petits systèmes et des petits systèmes qui fonctionnent en tant que terminaux satellites des gros ordinateurs et des réseaux informatiques. En outre, dans le cas des petits systèmes reliés aux gros ordinateurs ou aux réseaux informatiques, les normes de sécurité de «l'ordinateur central» doivent être respectées et, par conséquent, du «point de vue de l'ordinateur central», le petit système doit être conforme aux

1.2 Contexte

Il existe une grande différence entre l'utilisation des gros ordinateurs et des petits systèmes: la responsabilité et l'exploitation des premiers relèvent de la direction des centres de données, tandis que les usagers des seconds contrôlent tous les aspects de l'exploitation du système et en assument la responsabilité. Le personnel qui se sert de petits systèmes informatiques n'a habituellement aucune expérience en traitement de l'information et il ignore souvent jusqu'à quel point les petits systèmes sont vulnérables. Par conséquent, il peut arriver que les données de nature délicate contenues dans les petits systèmes ne soient pas adéquatement protégées.

Par le passé, la protection des gros ordinateurs, y compris la sauvegarde et le rétablissement des fichiers de données, incombaient au personnel des centres de données. Le vol de gros systèmes ou des périphériques connexes, par exemple les disques et les bandes, était peu fréquent, surtout à cause de la taille de ces systèmes et de la mise en place de mesures pour contrôler l'accès à la plupart des centres de données. Avec la prolifération actuelle des ordinateurs au bureau et à la maison, les petits systèmes sont exposés à un nouveau type de menaces. Le vol des composantes et des supports du système (disquettes et disques durs) n'est pas motivé par les données qu'ils contiennent mais par la valeur et l'attrait du matériel comme tel. Un autre point lié à l'utilisation des petits systèmes pose des problèmes sur le plan de la sécurité, surtout dans le cas des systèmes reliés à un réseau: la difficulté de contrôler l'expansion non autorisée du matériel et des logiciels risque de compromettre, accidentellement ou délibérément, la sécurité du système ou du réseau. En utilisant les petits systèmes informatiques, les usagers doivent

1. APERÇU

1.1 Introduction

La sécurité de la technologie de l'information (TI) est la protection qui découle d'un éventail intégré de mesures conçues pour assurer la confidentialité de l'information emmagasinée sur des supports électroniques, traitée ou transmise, l'intégrité de l'information et la disponibilité des systèmes et des services. Des normes de sécurité dans le domaine de la TI ont été élaborées afin d'aider les organismes gouvernementaux à mettre en oeuvre un programme efficace de sécurité de la TI. Le document intitulé «Normes de sécurité technique dans le domaine de la technologie de l'information (NSTTI)» traite des «composantes fondamentales de la sécurité», c'est-à-dire (1) la sécurité administrative et organisationnelle, (2) la sécurité du personnel, (3) la sécurité matérielle et du milieu, (4) la sécurité du matériel, (5) la sécurité des communications, (6) la sécurité des logiciels (7) et la sécurité des opérations. Les NSTTI décrivent en détail les exigences minimales en matière de sécurité auxquelles tous les systèmes informatiques doivent satisfaire pour protéger les données selon leur nature plus ou moins délicate.

Les lignes directrices énoncées dans les paragraphes qui suivent ont été extraites des NSTTI et modifiées de façon à tenir compte des nouvelles technologies utilisées dans les bureaux où l'on exploite de petits systèmes. Bon nombre de lignes directrices ne sont pas particulières à un environnement de ce genre, mais ont été regroupées ici à l'intention de l'usager.

Lignes directrices sur la sécurité des petits systèmes

Octobre 1992

Gendarmerie royale du Canada | Royal Canadian Mounted Police

En consultation avec d'autres...

Ce document fait partie d'une collection de publications sur la sécurité, publiée par les organismes conseils et les organismes centraux en consultation avec les ministères. La collection a comme but d'aider tous les ministères à répondre aux exigences et aux normes contenues dans la politique sur la sécurité et ses appendices.

Publié par la GRC en consultation avec :

Secrétariat du Conseil du Trésor du Canada
Centre de la sécurité des télécommunications
Comité de sécurité de la technologie de l'information

Ministre des Approvisionnements et Services Canada, 1992
Nº de cat. BT32-36/7 1992
ISBN 0-662-59297-2

ISSN 1188-6315
Publication en collaboration concernant la gestion d'information

Gouvernement du Canada

Sécurité

"Lignes directrices sur la sécurité des petits systèmes"

Canada